VeriSign™

New Hampshire Department of Consumer Affairs
Attn: Mary Gould
33 Capitol Street
Concord, NH 03301

July 27, 2007

Dear Ms. Gould:

The purpose of this letter is to notify the department of consumer affairs that VeriSign, Inc., has sustained a possible loss of personal information of certain of its current and former employees, between the evening of Thursday, July 12, 2007 and the morning of Friday, July 13, 2007. This incident occurred when a laptop possibly containing some personal information was stolen from an employee's vehicle which was parked in her garage. The personal information on the laptop, if any, would have included name, Social Security number, date of birth, and salary information, but did not include any credit card numbers, bank account numbers, or password information.

When VeriSign was notified of this matter on Friday, July 13, we initiated an internal investigation and also asked the Sunnyvale, California Police Department to investigate. We also began preparations to notify all affected individuals of the loss and its potential impact upon their credit.

Attached is a copy of the notification sent to current US employees, together with an FAQ. Similar notifications were sent to affected former US employees and affected international employees. Please contact me at the phone number or address indicated below in the event that you have questions regarding this matter, or desire further information regarding the status.

Sincerely,

Rebecca Matthias

Rebecca Matthias
Director, Legal
VeriSign, Inc.
487 East Middlefield Road
Mountain View, California 94043
Tel. 650.426.5117
Email – rmatthias@verisign.com

Dear VeriSign Employee:

The purpose of this letter is to inform you that a laptop possibly containing VeriSign employee information was stolen from the vehicle of a VeriSign employee, while parked in the employee's Northern California garage between the evening of Thursday, July 12, 2007, and the morning of Friday, July 13, 2007. The laptop possibly contained personal information including name, Social Security number, date of birth, and salary information, but it did not include credit card numbers, bank account numbers, or password information. The laptop did not contain any information about any VeriSign customers.

This note has two communications objectives: 1) To let you know what VeriSign is doing out of the abundance of caution to alert employees and former employees and share what resources we are offering to help you; and 2) to underscore the importance of protecting sensitive and proprietary information.

First, we are contacting all individuals whose personal information may have been on the stolen laptop. We have no reason to believe that the thief or thieves acted with the intent to extract and use this information; the police have indicated that there may be a connection to a series of petty thefts in the neighborhood. The laptop was fully shut down and requires a user name and password to log on to the Windows application. To our knowledge, the thieves do not have the password.

Investigation of the Incident
When we learned of this matter, we immediately initiated an internal investigation and also ensured that the police were contacted to investigate the matter. We will continue to cooperate with law enforcement as they investigate this matter. In accordance with applicable law, we had to first notify and work with law enforcement before we were permitted to notify you.

VeriSign Information Security Policy
VeriSign already has a strong Information Security Policy in place, which in this case was unfortunately not followed. VeriSign's Information Security Team issues a quarterly publication to remind employees of this policy. For this incident, we disabled any access by the employee's computer to the VeriSign network or any information located on the VeriSign network, going forward, and we are reviewing our security procedures to help prevent a recurrence of this type. Among other things, we plan to implement procedures to more strictly enforce our policy of encrypting sensitive data stored on company computers.

This incident should serve as a reminder to all of us never to leave our laptops in plain view in a car, to avoid storing sensitive data on our laptops' hard drives if at all possible, and to use data encryption tools to protect those sets of data that we absolutely must have stored on our laptops. These guidelines are set forth in Section 5.5.6 of the VeriSign Information Security Policy.

What You Can Do Now
U.S. residents have rights under U.S. law to place a "fraud alert" on their credit file, which alerts creditors to take additional steps to verify their identity prior to granting credit in their name. You can place a fraud alert on your credit file yourself by calling just one of the three nationwide consumer reporting agencies which are listed below. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

Equifax: 1-800-525-6285; www.equifax.com
Experian: 1-888-397-3742; www.experian.com
TransUnion: 1-800-680-7289; www.transunion.com
U.S. residents are also entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, you can visit www.annualcreditreport.com or call toll-free (877) 322-8228. For additional information on how to further protect your personal information, you can visit the web site of the U.S. Federal Trade Commission at www.consumer.gov/idtheft/ or at www.ftc.gov/idtheft.

What VeriSign is Doing to Prevent Abuse of Potentially Compromised Information
We deeply regret that this has happened. Although we do not have information that any of the personal information has been misused, we are committed to making sure you have the support you need to monitor your credit and know how to respond if you identify any problems.

In particular, to assist you, we have arranged with Equifax to help you protect your identity and your credit information. To receive this service, you will need to enroll in the Equifax Credit Watch™ Gold with 3-in-1 Monitoring service. The details on how to enroll in this service will be provided to you in a separate email to follow shortly. This product is being provided to you for 12 months at no cost to you.

We strongly encourage you to take advantage of our offer to enroll with Equifax, and to remain vigilant by reviewing your account statements and monitoring your credit report frequently.

We are also asking all of our employees to familiarize themselves with the Information Security Policy and always be mindful of protecting sensitive information.

If you have any questions or concerns, please review the FAQs that we have prepared related to this incident and feel free to contact DataSecurity@verisign.com.

Sincerely,

VeriSign Corporate Human Resources

VeriSign Confidential – Do Not Forward

Laptop Theft FAQ
U.S. Employees Version
As of July 23, 2007

What theft occurred?
A VeriSign-issued laptop was stolen from an employee's vehicle parked in her garage between the evening of Thursday, July 12, and the morning of Friday, July 13, 2007. The laptop may have contained some information about current and certain former employees, which may have included name, Social Security number, date of birth, and salary information, but did not include any credit card numbers, bank account numbers, or password information.

Do you think the theft was specifically to steal personal identity information?
We have no reason to believe that the thief or thieves acted with the intent to extract and use this information. The local police have said the theft may be tied to a series of neighborhood burglaries. Also, the laptop was fully shut down and requires a user name and password to log into the Windows application. To our knowledge, the thieves do not have the password. Regardless, we felt it was important to alert employees given the possibility of personal information being on the laptop.

Were the police called?
When VeriSign was notified of this matter on Friday, July 13, we immediately initiated an internal investigation and ensured that the Sunnyvale, California Police Department was contacted to investigate the incident. We have also contacted law enforcement in other areas where individuals are affected. We will continue to cooperate with law enforcement as they investigate this matter. In accordance with applicable law, we had to first notify and work with law enforcement before we were permitted to notify affected individuals.

What types of information were on the laptop?
The laptop may have included personal information of current and some former VeriSign employees including name, Social Security number, date of birth, and salary information, but it did not include any credit card numbers, bank account numbers, or password information.

Was there any information on employees' dependants on the laptop?
No.

Was there any customer information on the laptop?
No.

What can current and former employees do to protect themselves?
U.S. residents have rights under U.S. law to place a "fraud alert" on their credit file, which alerts creditors to take additional steps to verify their identity prior to granting credit in their name. You can place a fraud alert on your credit file yourself by calling just one of the three nationwide consumer reporting agencies which are listed below. As

soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

Equifax: 1-800-525-6285; www.equifax.com
Experian: 1-888-397-3742; www.experian.com
TransUnion: 1-800-680-7289; www.transunion.com

U.S. residents are also entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order the free credit report, you can visit www.annualcreditreport.com or call toll-free (877) 322-8228. For additional information on how to further protect your personal information, you can visit the web site of the U.S. Federal Trade Commission at www.consumer.gov/idtheft/.

Who can I contact if I have additional questions?
Email DataSecurity@verisign.com.

What is VeriSign doing to help affected individuals?
Although we do not have information that any of the personal information has been misused, we are committed to making sure current and former employees whose personal information may have been on the stolen laptop have the support they need to monitor their credit and know how to respond if they identify any problems.

In particular, to assist current and former employees, we have arranged to provide current and former VeriSign employees whose personal information may have been on the stolen laptop with Equifax Credit Monitoring service to help them protect their identity and credit information at no cost to them for a period of 12 months. Enrollment details will be mailed to affected individuals shortly.

We strongly encourage you to take advantage of our offer to enroll with Equifax, and to closely review your account statements and monitor your credit report frequently.

Does VeriSign have a policy about storing employee information on laptops?
Yes, VeriSign has a policy on how to manage laptops that include sensitive information and company data. That policy includes not leaving laptops in vehicles in plain view, keeping the amount of confidential and sensitive data stored on laptops to a minimum, and using data encryption tools to protect those sets of data that absolutely must be stored on a laptop. VeriSign's Security Department issues a quarterly publication to remind employees of this policy. Unfortunately the policy was not completely followed in this case. See VeriSign's Information Classification and Handling Standard for more information.

What is VeriSign Doing to prevent this from happening again?
VeriSign already has a strong Information Security Policy in place, which is accessible to all employees. For this incident, we disabled any access by the employee's computer to the VeriSign network or any information located on the VeriSign network. Going forward, we will continue to review our security procedures and actively communicate them to employees, so we can prevent future human errors of this type. In particular, we are looking to implement more procedures that reinforce our policy of encrypting sensitive data stored on company computers.

This incident should also serve as a reminder to all of us never to leave our laptops in

plain view in a car; to avoid storing sensitive data on our laptops' hard drives if at all possible; and to use data encryption tools to protect those sets of data that we absolutely must have stored on our laptops. For more information, VeriSign employees can refer to Section 5.5.6 of the VeriSign Information Security Policy.